USAID
FROM THE AMERICAN PEOPLE

ADS Chapter 565

Physical Security Programs (Domestic)

Document Quality Check Date: 10/04/2012
Full Revision Date: 05/24/2012
Responsible Office: SEC/ISP
File Name: 565_100412

Functional Series 500 - Management Services
ADS 565 - Physical Security Programs (Domestic)
POC for ADS 565: David Blackshaw, (202) 712-1259, DBlackshaw@usaid.gov

This chapter has been revised in its entirety.

Table of Contents

ADS Chapter 565 - Physical Security Programs (Domestic)

565.1 OVERVIEW

Effective Date: 05/24/2012

This chapter provides the policy directives and required procedures for the protection of USAID/Washington (USAID/W) employees and national security information in USAID headquarters buildings and offsite facilities.

565.2 PRIMARY RESPONSIBILITIES

Effective Date: 05/24/2012

a. The **Director, Office of Security (SEC/OD)** provides centralized security support to the Agency, with the exception of unclassified automated systems security. S/he supervises, directs, and controls all security activities relating to the programs and operations of USAID. S/he serves as the Agency's Senior Security Official and advises the Administrator and USAID senior staff on all security matters. (See **ADS 101, Agency Programs and Functions,** and **ADS 103, Delegations of Authority**.)

b. The **Division Chief, Office of Security, International Security Programs (SEC/ISP)** implements physical security programs in USAID headquarters buildings, offsite facilities, and overseas missions.

c. The **Director of the Bureau for Management, Office of Management Services (M/MS)** ensures that SEC is apprised of future relocations of USAID personnel and assets and (in advance if possible) of any matters affecting the operations of physical security systems in USAID headquarters buildings and offsite facilities.

d. **USAID Senior SEC Managers**, Division and Branch Chiefs, ensure staff compliance with the security policy directives and required procedures contained in this chapter.

e. The **Domestic Security Branch Chief (SEC/ISP/DS)** ensures staff compliance with the security policy directives, physical security programs, guard force, and required procedures contained in this chapter and Homeland Security Presidential Directive-12 (HSPD-12).

f. The **AMS Officer** within the Office of Security plays an integral role in ensuring HSPD-12 compliance is strictly adhered to. The AMS officer, as the authorized sponsor within SEC, reviews all initial requests submitted by personnel for a Federal Identification Card (PIV)/Facility Access Card (FAC).

g. **All individuals** must comply with the security policy directives and required procedures contained in this chapter.

565.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

565.3.1 USAID Headquarters Building Security Standards

Effective Date: 05/24/2012

The USAID headquarters building is designated as a Level IV facility, as defined in the Interagency Security Committee (ISC) Standards Report, dated April 12, 2010, which supersedes the U.S. Department of Justice Vulnerability Assessment of Federal Facilities Report (June 28, 1995). The physical security standards specified in this report apply to the USAID headquarters building (Ronald Reagan Building) and offsite locations (SA-44, SA-41, COOP Site, and Potomac Yards II). (See **Interagency Security Committee Standard: Physical Security Criteria for Federal Facilities, April 12, 2010**.)

565.3.2 Designated Restricted and Unrestricted Areas

Effective Date: 05/24/2012

All office space within USAID/W headquarters and offsite facilities are designated as either “restricted” or “unrestricted” space. A change in designation for any office or office suite must be requested in writing by the B/IO Assistant Administrator or Office Director and sent to SEC/CTIS. Subsequent approval or disapproval by SEC/CTIS is based upon an inspection and evaluation of the space to determine and ensure full compliance with established standards. SEC/CTIS maintains a listing of all restricted and unrestricted office space.

Designated restricted space is defined as an area where storage, processing, discussions, and handling of classified material may occur. Designated restricted areas are authorized for classified equipment such as stand-alone computers, ClassNets, and STU/STE equipment.

Upon request, SEC may grant unescorted access to designated restricted space to an authorized individual who has a valid national security clearance at the “Secret” level or higher. The security clearance must be properly certified and forwarded to SEC in writing by the individual’s parent agency or organization. Other personnel requesting access to designated restricted space must be escorted by a cleared, authorized employee that has been granted “unescorted access” to the designated restricted area.

Unrestricted space is defined as an area where storage, processing, discussion, and handling of classified material are not authorized. Classified meetings or conversations are not authorized in designated unrestricted areas.

Upon receiving a written request by the individual's AMS officer, SEC may grant access to "unrestricted areas" to any authorized person(s) that has received a favorable background investigation as determined by SEC. Authorized persons include:

- U.S. Direct Hire Employees;
- Personal Services Contractors; and
- Cleared (under reciprocity) Foreign Nationals for Facility Access

All USAID overseas Missions are designated as unrestricted and prohibited from storage and processing of classified information. All classified information must be stored, processed, and discussed in the Controlled Access Area (CAA) inside the U.S. Embassy, as designated by the Regional Security Officer (RSO). (See **ADS 562.3.1**)

565.3.3 Access to and Within USAID Headquarters and Offsite Facilities

565.3.3.1 Authorization to Work in USAID Headquarters and Offsite Facilities

Effective Date: 05/24/2012

Only those individuals who have been the subject of a background investigation and have received a favorable review by SEC are permitted to work within USAID space and be issued a USAID headquarters Personal Identity Verification (PIV) Card or Facility Access Card (FAC) to access USAID government space.

- Individuals with a current security clearance verified by SEC are authorized to work within USAID designated restricted areas. Individuals with an appropriate background investigation verified by SEC are authorized to work within USAID designated unrestricted areas.

- Visitor passes (see **565.3.4**) must not be requested or used for people to work in USAID space unless pre-approved by authorized SEC personnel. Exceptions are granted on a case-by-case basis and must be approved by the Domestic Security Branch Chief or ISP Division Chief, or designated staff acting on their behalf.

- SEC must specifically pre-approve unescorted access to work in unrestricted areas by individuals without a security clearance. This includes unescorted access by USAID Foreign Service Nationals (FSN) and Third Country Nationals (TCN) on temporary duty (TDY) to USAID/W headquarters, and contractors' employees working temporarily in USAID space. The Bureau/Independent Office (B/IO) AMS Officer must submit a request for such authorization to SEC/ISP/DS via an emailed memo to **SECDomestic@usaid.gov** at least one full week in advance of the

proposed work date. A concise and brief security plan must specify what measures have been implemented to safeguard national security information from unauthorized access by an uncleared person. The request must include the following information:

1. The purpose of the visit (training, etc.).
2. The office and location where the visitor (e.g., FSN/TCN PSC or contractor employee) will be assigned.
3. The identity of the USAID employee who will be the primary point of contact for administrative matters pertaining to the visitor.
4. The dates of visit.
5. Statement that the visitor will not have access to any classified information and to restricted space.

SEC will base approval on its assessment of the adequacy of the proposed measures.

- SEC/DS will coordinate with the FSN/TCN/or contractor employees assigned Mission and RSO to validate required background checks and facility access requirements were completed prior to authorizing the issuance of a USAID HSPD-12 Facility Access Card (FAC).

- The AMS officer for the sponsoring bureau must submit a 500-1 Badge Request Form to SEC/ISP/DS via the **SECDomestic@usaid.gov** e-mail box, once this cursory background check has been completed.

565.3.3.2 Obtaining a USAID Headquarters Federal ID/Personal Identity Verification (PIV) Card or Facility Access Card (FAC), and Reissuance of Credentials

Effective Date: 05/24/2012

Individual USAID Direct Hires, Personal Service Contractors, employees of Private Industry Contractors and other Government entities, including Congress, must be sponsored by a USAID B/IO to obtain a Federal ID/PIV or Facility Access Card (FAC).

The sponsoring office must coordinate the request for a building pass for congressional personnel with the Bureau for Legislative and Public Affairs (LPA) and the Office of the Executive Secretariat (ES) before SEC will process the request.

To obtain physical access to USAID/W or a Federal ID card issued under **Homeland Security Presidential Directive-12 (HSPD-12)**, AMS Officers must forward a completed **AID Form 500-1, Request for Federal Identification Card/Facility Access Card** to the "SEC Badges" (**SECDomestic@usaid.gov**) mailbox. It is the responsibility of the requesting B/IO AMS Officer to determine

and specify the access level required by the individual(s).

For contractor employees, the sponsoring B/IO AMS must coordinate with their company's Facility Security Officer (FSO) and comply with the HSPD-12 requirements to obtain a Facility Access Card for them.

Before individuals are granted unescorted access to government facilities, all requirements of **HSPD-12** must be met. These requirements are as follows:

- Favorable adjudication of clearance or background investigation;
- Sponsorship by AMS, OHR, or other proper authority;
- Completion of in-person enrollment/identity proofing. An employee or contractor is issued a credential only after presenting two identity source documents to the Enrollment Office (M/CIO), at least one of which must be a valid Federal or State government issued picture identification. See HSPD-12 and reference to the **Form I-9, Employment Eligibility Verification**, for a complete list of acceptable documents as proof of identification.
- Attendance at appropriate SEC security briefing; and
- Authentication by the Badge Office.

Pursuant HSPD-12 policies, a cardholder must be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV/FAC Card and until the actual expiration of the card. The expired PIV/FAC Card must be returned to SEC/ISP/DS for proper deactivation and destruction.

A cardholder must apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of an employee status or attribute change.

All requests for physical access or the issuance of a Federal PIV/FAC Card are reviewed and subject to approval by SEC.

Personnel who are posted abroad whose PIV/FAC Card is within three months of expiration and plan to be in the Washington, DC area either during home leave or TDY should notify their AMS officers to arrange for a badge renewal while in the DC area. The Domestic Security Branch will accommodate individuals in this category.

565.3.3.3 Use of USAID Headquarters Federal ID/Personal Identity Verification (PIV) Card or Facility Access Card (FAC)

Effective Date: 05/24/2012

All individuals within the USAID headquarters and offsite locations must possess and wear a valid USAID Federal ID/Personal Identity Verification (PIV) Card, Facility Access Card (FAC), or visitor pass at all times, regardless of employment type.

- All individuals must wear the Federal ID/PIV Card or FAC Card on the outer garment on the upper torso front with the front of the pass clearly visible.
- The Federal ID or FAC Card must not be altered (e.g., affixed with stickers, pins, or other items) in any way.
- All individuals are prohibited from lending building passes or ID cards to other employees or visitors.
- Federal ID cards must be used only for official business purposes.
- All individuals should conceal their card after departing USAID Headquarters and offsite facilities.
- SEC will make exceptions to the mandatory pass rule for children under the age of 17 and for those visitors whose range of movement is severely limited who are attending a USAID function.

565.3.3.4 Access to Offices and Suites Within USAID Headquarters and Offsite Facilities

Effective Date: 05/24/2012

Authorized personnel may have access to rooms/suite entry door within USAID space only after coordination/endorsements from their servicing AMS Officer, the AMS officer of the space in question, and SEC.

Requests for access to office space within AID/W must be submitted by the sponsoring B/IO AMS Officer to the “SEC Badges” (**SECDomestic@usaid.gov**) mailbox. All requests must include the following:

- The individual’s name,
- Door or suite number requested,
- Time of day requested (shift name), and

- The purpose of access.

Requests for access to another B/IO space must also include approval from the AMS Officer of the space in question. SEC will notify the AMS Officer when the requested access changes are completed.

Hours of access to suite entry doors and turnstiles within USAID are defined as follows:

Always = 24 hours a day, seven days a week, holidays included;
Flex = 6:30 a.m. to 6:30 p.m., five days a week, no holidays or weekends;
Core = 8:45 a.m., to 5:30 p.m., five days a week, no holidays or weekends; and
Vendor = 7:30 a.m. to 3:30 p.m., five days a week, no holidays or weekends.

Access to freight elevators, GSA doors, and specific secured areas is granted on a case-by-case basis. To obtain access, follow the same procedures (above) for requesting access to a door or suite. Access to these areas may require additional time for approval and processing.

565.3.3.5 Access to Offices Within USAID Space at SA-44 (Federal Center Plaza)

Effective Date: 05/24/2012

Authorized personnel may have access to USAID space within SA-44 space only after coordination/endorsements from their servicing AMS Officer, the AMS officer of the space in question, and SEC have been established and accepted.

Requests for access to office space within SA-44 must be submitted by the B/IO AMS Officer to the "SEC Badges" (**SECDomestic@usaid.gov**) mailbox. All requests must include the following:

- The individual's full name,
- Door or suite number requested,
- Time of day requested (shift name), and
- The purpose of access.

Requests for access to another B/IO space must also include approval from the AMS Officer of the space in question. SEC will notify the AMS Officer when the requested access changes are complete.

Hours of access to suite entry doors within SA-44 are defined as follows:

Always = 24 hours a day, seven days a week, holidays included;
Flex = 6:30 a.m. to 6:30 p.m., five days a week, no holidays or weekends;
Core = 8:45 a.m., to 5:30 p.m., five days a week, no holidays or weekends; and
Vendor = 7:30 a.m. to 3:30 p.m., five days a week, no holidays or weekends.

Pursuant Department of State (DoS) policy, DoS and USAID employees entering Federal space within SA-44 are required to sign in only during non-flex hours and during weekends. Employees must have their PIV Card in possession in order to be allowed access during these times.

Access to freight elevators and specific secured areas is granted on a case-by-case basis and must be coordinated with the Facilities Manager, Bureau for Management, Office of Management Services, Headquarters Management Division (M/MS/HMD). The Facilities Manager is responsible for coordinating with the property manager at the facility. To obtain access, follow the same procedures (above) for requesting access to a door or suite. Access to these areas may require additional time for approval and processing by SEC.

For access to Potomac Yards II freight elevators and specific secured areas, the Office of Security, Domestic Security Branch coordinates all requests directly with the U.S. Environmental Protection Agency (EPA), Office of Administration and Resources Management, Security Management Division, Security Operations Branch, since EPA is the primary tenant at this building.

565.3.3.6 TDY Badges

Effective Date: 05/24/2012

Overseas employees and USPSCs with at least secret level security clearance on Temporary Duty Assignment (TDY) in USAID/W may obtain a TDY badge at the Ronald Reagan Building's (RRB's) 14th Street Visitor Control Desk. After verification of the individual's identity, employment status, clearance level, and sponsoring B/IO, a TDY badge will be issued for the duration of the TDY assignment.

FSN/TCN PSCs and USPSCs without at least a secret level clearance must show their embassy-issued identification card at the RRB Visitor Control Desk before being issued an un-cleared TDY badge or Facility Access Card (FAC).

When an employee on TDY is assigned to SA-44 or Potomac Yards II, their respective AMS Officer is required to notify **SECDomestic@usaid.gov** prior to the employee's arrival to arrange for the issuance of a temporary badge. The AMS Officer should also notify the Security Officer at SA-44 or Potomac Yards II to facilitate the employees' access and preclude possible delays.

To expedite the verification process, the sponsoring office (normally the B/IO AMS Officer) must send an e-mail to the Office of Security mailbox (**SECDomestic@usaid.gov**), which includes the following:

- The individual's full name,
- Start and end dates of the TDY,
- Mission location,
- Clearance level, and
- The sponsor's contact information.

TDY badges will enable individuals to proceed unescorted through the turnstiles at the Ronald Reagan Building's 13 ½ and 14th Street lobbies into USAID space. The pass also permits the individual to enter USAID space that is approved for the clearance level of the TDY pass holder. AMS Officers may request that additional access be added to the TDY badge by following the procedures in **565.3.6**. Requests to add access to a TDY badge must also include the TDY badge number (located on the front of the card).

Individuals must return all TDY passes to the Visitor Control Desk upon completion of the TDY assignment.

The B/IO AMS Officer should request a permanent photo building pass for any individual scheduled for TDY in USAID/W for more than ten (10) working days. Such requests must be submitted on an **AID 500-1** and sent electronically to the "SEC Badges" (**SECDomestic@usaid.gov**) mailbox. All requests for physical access to government space are subject requirements of **HSPD-12**.

Any individual assigned to any of the USAID/W facilities for more than 30 days must obtain an HSPD-12 issued badge**.**

565.3.3.7 Temporary Badges

Effective Date: 05/24/2012

Individuals required to have access to USAID/Washington facilities who report to work without their authorized Federal ID card/FAC must request a temporary badge (T-Badge). Uniformed guards are required to verify the identity of the individual before issuing the T-badge. T-badges are not issued to any individual with an expired Federal ID card. Unless special authorization is approved by SEC, a T-badge will be issued for a period of one day.

Individuals required to have access at the Ronald Reagan Building must request a T-Badge from the 14th Street Visitor Control Desk.

Individuals required to have access to SA-44 must request a T-Badge from the

U.S. Department of State Front Desk Officer, upon approval by the USAID Security Officer.

Individuals required to have access to Potomac Yards II must report to the EPA Front Desk Security Officer at Potomac Yards II to request a T-Badge. The individual will be required to contact a direct hire employee to serve as an escort. The uniformed guard is required to verify the identity of the individual before issuing a T-badge.

An individual's regular Federal ID card/FAC will be deactivated until his/her T-badge is returned. Individuals are prohibited from using multiple badges simultaneously (i.e., temporary or TDY badge and photo HSPD-12 ID).

565.3.3.8 Procedures for VIP Visits

Effective Date: 05/24/2012

USAID employees who expect to receive VIP visits by heads of state/government, reigning royalty, or cabinet-level guests must submit the following information to the respective SEC and LPA email mailboxes noted below at least 48 hours prior to the visit to ensure compliance with protocols regarding processing and access. The USAID employee must send an email to **SECVIP@usaid.gov** and **SpecialEvents@usaid.gov** and include the following information:

- Identity of the designated escort officer and provide contact information;
- Sponsoring bureau or office, telephone number, and the names(s) and titles(s) of each member of the VIP delegation (including prefix, full name and title);
- Prefixes, names, and titles of any other accompanying U.S. government personnel; and
- Date, time, and meeting room.

On the day of the visit, the employee who will provide escort must re-confirm two hours prior to the visit to **SpecialEvents@usaid.gov.** A "VIP Escort Badge" will be subsequently issued to the escort, who must sign out the badge at the 14th Street Visitor Control Desk, after confirmation has been received from **SECVIP@usaid.gov** and **SpecialEvents@usaid.gov.**

The USAID Bureau for Legislative and Public Affairs (LPA) will determine if the visitors fall within the accepted categories for VIP protocol. LPA handles logistics (flags, photos, gifts, escorts, internal press coverage, etc.), as appropriate to the rank of the guest.

565.3.3.9 Replacement of Federal PIV/FAC Badges

Effective Date: 05/24/2012

Individuals required to have access to USAID/Washington facilities must immediately report any lost, compromised, or possibly stolen Federal PIV or FAC badge to their AMS Officer, or immediate supervisor, and the SEC Main Desk at (202) 712-0990. The individual may request a replacement badge by completing the **AID 500-1**. The **AID 500-1** must be submitted electronically to the "SEC Badges" (**SECDomestic@usaid.gov**) mailbox by the AMS Officer. Individuals must wait a minimum of five working days for authorization for a replacement badge. A temporary badge will be issued by SEC in the interim.

Individuals must submit a written statement to their AMS Officer and immediate supervisor detailing the facts and circumstances of the loss, theft, or compromise, including all actions taken to recover the lost badge. This letter must be attached to the **AID 500-1 Form**, when submitted to the SEC Badges mailbox for lost badge replacement.

Individuals requesting replacement due to physical damage or failure of a Federal PIV or FAC badge are subject to all requirements for enrollment, identity proofing, and authentication under the **HSPD-12** program.

565.3.3.10 Required Verification of Federal ID (PIV) Card/ Facility Access Card (FAC)

Effective Date: 05/24/2012

Uniformed guards are required to positively identify individuals with badges by examining the photograph on the front of the badge. All employees must cooperate with the identification process. If the employee does not resemble the photograph on the badge, the uniformed guard may request the employee report to the Badge Office for an updated photograph. Employees who do not comply will have their building access suspended until a replacement PIV/FAC badge is obtained.

565.3.3.11 Return of Federal ID (PIV) Card/Facility Access Card (FAC)

Effective Date: 05/24/2012

An employee must return his/her Federal ID (PIV) Card or Facility Access Card (FAC) at the end of the day when

- That employee leaves the Agency, or
- That employee is no longer working under the employment mechanism in which they applied for and received the building pass or Federal ID card/Facility Access Card.

All cards must be returned to SEC prior to an employee's departure.

- U.S. Direct Hires and Personal Services Contractors (PSCs): Employees are required to return their identification cards to SEC during the mandatory security debriefing and employee "check out" procedures.

- Uncleared Institutional Contractors and Detailees: The Agency sponsor (B/IO AMS Officer) is responsible for collecting the identification cards from employees at the conclusion of the contract or detail.

- Cleared Institutional Contractors: The Contracting Officer's Representative (COR) is responsible for ensuring that the FSO for the parent company returns the identification cards to SEC at the conclusion of the contract or when the employee is no longer working under the mechanism in which the card was issued.

- USAID badges may be returned via mail to:

  USAID/SEC/ISP/DS
  RRB Room B. 2.6-32A
  1300 Pennsylvania Avenue, N.W.
  Washington, DC 20523

565.3.3.12 Confiscating Invalid Federal ID Cards

Effective Date: 05/24/2012

The security guards posted at USAID/Washington facilities will confiscate any expired or invalid Federal ID card/FAC card. Individuals requiring access to these facilities whose badge has been confiscated must notify the USAID Security Badge Office to report the circumstances. These individuals may request the issuance of a T-Badge. The B/IO AMS Officer must complete a new **AID 500-1** to request re-issuance of a new card.

Security officers at the Ronald Reagan Building USAID turnstiles and at SA-44 are authorized to confiscate any expired Federal ID card/FAC card.

The security officers at PYII are authorized to confiscate any expired Federal ID card/FAC card and will return the card to USAID SEC.

565.3.4 Visitors and Guests to USAID/W

Effective Date: 05/24/2012

USAID employees who expect to receive visitors at USAID/W are required to pre-register their sponsorship of the visitor via the Visitor Registration System (VRS). Employees can access the system via the AIDNET by clicking the Visitor Registration System ICON and accessing the system. When a visitor checks in at the USAID Front Desk and furnishes a valid, government-issued photo

identification (driver's license, U.S. government-issued ID card, U.S. passport, State Department ID), a personalized visitor's pass will be issued to the visitor. The pass will note the visitor's name, date of visit, and sponsor's name. The USAID sponsor will be automatically notified of the visitor's arrival by e-mail and also receive telephonic notification to provide an escort.

Non-U.S. citizens must be pre-registered at least five (5) days in advance in order to process the request and furnish a valid foreign passport upon arrival when checking in.

USAID employees at SA-44 may notify the SA-44 Security Officer of visitors and provide their names in advance to facilitate their access. This information will be subsequently forwarded to DoS Diplomatic Security and the Front Desk to facilitate the process. Employees expecting to receive groups of five (5) or more visitors are required to notify the SA-44 USAID Security Officer at least two days in advance to allow DoS sufficient time to process their screening access.

All visitors and guests must present a valid (un-expired) identification before they may enter USAID space in the Ronald Reagan Building (RRB) or any USAID offsite facility.

Additionally, visitors and guests, excluding Department of State employees with proper State issued identification, will be subject to metal detection and package screening before entering USAID space.

When uncleared individuals, such as building construction contractors, are required to enter or remain in the building after working hours, the direct-hire employee from the sponsoring B/IO authorizing the work must arrange for an escort and obtain SEC concurrence. Such individuals must:

- Sign in and out on the appropriate register designated by SEC,
- Wear visitor's passes for the duration of the visit, and
- Surrender visitor's pass at the 14th Street Visitor Control Desk when leaving USAID space for the day at the Ronald Reagan Building.
- Surrender visitor's pass at the Front Visitor's Desk when leaving USAID space for the day at SA-44 or PYII.

The B/IO escort is responsible for ensuring visitors comply with appropriate sign in/sign out procedures.

USAID employees who escort or approve the admittance of an individual are responsible for the individual's compliance with the pass requirements and his or her prompt departure from the building immediately following completion of their

business. Visitors must be escorted by the escort official or sponsor at all times while in USAID space for the duration of their visit, with the exception of visits to common area restrooms.

Employees who fail to comply with escort procedures and policy will be cited for each violation. When an employee is cited three times for not following the established escort procedures and policy, SEC will revoke their escort privileges. The employee will be required to surrender their current badge annotated with the "E" designation on the front of the badge, and they will then be reissued a replacement badge with no escort privileges. Violations of a security regulation may lead to disciplinary and adverse actions under **ADS Chapter 487, Disciplinary and Adverse Actions Based Upon Employee Misconduct – Civil Service** and **ADS Chapter 485, Disciplinary Action – Foreign Service**.

565.3.5 Access to Domestic Department of State Building Facilities (Physical Access) for USAID Employees

Effective Date: 05/24/2012

Access to domestic Department of State facilities may be added to Federal ID or Facility Access (FAC) cards. SEC only sponsors access to Main State (HST Building) on Federal ID cards. All other requests for access to State facilities must be requested directly from the State Department sponsor or Unit Security Officer by the employee or B/IO AMS Officer.

565.3.6 Use of Cameras, Photographic or Video Teleconferencing Equipment, Personal Digital Assistants (PDAs), Smartphones, and Bluetooth Devices

Effective Date: 05/24/2012

The use of cameras or photographic equipment is not permitted within restricted space in the USAID portion of the Ronald Reagan Building (RRB) and offsite facilities. This restriction does not apply to the public portion of the USAID Public Information Center on the Mezzanine level. A camera is defined as any personally owned still, motion, or video recording device, including cell phones with a camera feature and cameras attached to computer equipment. This does not preclude personnel from possessing their cell phones while in these areas, only the use of them for taking photographs.

Requests to waive the camera restriction may be granted on a case-by-case basis by SEC for special occasions and ceremonies. The request must be sent to the SEC Badge Office (**SECDomestic@usaid.gov**) mailbox at least two full business days prior to the day of the planned use. The request must include the following:

- The identity of the person bringing the camera;
- The make and model of the camera;

- A description of where the photographs will be taken; and
- The intended subject and purpose of the photographs.

SEC will provide guidance on inspecting the location prior to the event to ensure that no classified or sensitive but unclassified (SBU) information is visible. The requestor is responsible for completing the inspection prior to the arrival of guests.

Members of visiting official delegations and credentialed media representatives may bring cameras into USAID space after approval from LPA and coordination with SEC. The event sponsor must coordinate with LPA's Press Office no less than one full business day before the planned event. LPA will notify SEC when the request has been approved.

In cases where advance notification is not possible, (e.g., a breaking news story) LPA must contact SEC directly by calling SEC's Main Desk at (202) 712-0990 to coordinate and authorize camera usage.

The installation and/or use of video teleconferencing equipment, Web cameras, or other devices which transmit audio or video is prohibited unless approved in advance by SEC. All requests for exception must be presented to SEC in writing. Written requests must be directed to the attention of the SEC's Chief, Counterterrorism, Information Security Division. Requests must include the following:

- A description of the equipment, including all specifications;
- The location where the equipment will be installed;
- The proposed uses for the equipment;
- A point of contact;
- A security plan (if inside a designated restricted area); and
- Approval from M/CIO, where applicable.

Employees are responsible for ensuring that visitors understand and comply with USAID's camera use policy.

Moreover, the transport and/or use of cameras, personal digital assistants (PDAs), and smartphones are prohibited in Sensitive Compartmented Information Facility (SCIF) areas. The use of Bluetooth devices within USAID facilities is also prohibited. (**ADS 545, Information Systems Security**, states

"users must not use modems, Bluetooth, or other wireless devices unless CISO approved.")

565.3.7 Alteration of Security Systems or Locks

Effective Date: 05/24/2012

Unauthorized modifications (i.e., propping open doors) or other action(s) without written consent from SEC, which may adversely affect the operation of the physical security measures/system at USAID headquarters and offsite facilities, will result in SEC recommending the Agency take appropriate disciplinary action against the responsible violator.

Employees are not permitted to attach any device(s) or modify any aspect of USAID's access control system, including card readers, motion detectors or alarms. Bureau/Independent Offices (B/IOs) are prohibited from securing the services of any security contractor to alter the Agency's access control system or install or alter any locks, even when part of a construction project. Written authorization from SEC must be obtained before any part of a building's security system, or any security locking device used for the protection of National Security Information, is modified or disengaged.

565.3.8 Safe and Door Combination Control

Effective Date: 05/24/2012

SEC maintains a master listing of all USAID safe combinations and Unican door combinations. The Administrative Management Officer (AMS) in each B/IO must maintain a list of the security container (safe) combinations and Unican door combinations in a safe for his or her B/IO. The AMS must ensure that no unauthorized person gains access to these combinations.

Only authorized SEC personnel may change door and safe combinations, unless SEC grants an exception due to exigent circumstances. When an individual having knowledge of a safe combination changes employment with the respective B/IO, the AMS must notify SEC and arrange to have the combination(s) changed.

The AMS must notify SEC immediately if a B/IO safe combination is believed to have been compromised. The reporting B/IO must provide relevant information concerning the incident to permit an investigation and arrange to have the affected combination changed.

565.3.9 Property Passes

Effective Date: 05/24/2012

Employees leaving USAID space with sealed packages, boxes, luggage, or

government equipment must provide the uniformed guard with a valid property pass signed and dated by their designated AMS Officer, or his/her designee. Employees/contractors removing personal property such as laptop computers, monitors, luggage, etc. that might appear to be government equipment must be able to prove ownership and be in possession of a properly completed USAID property pass. **(See GSA Optional Form 7).** Whether a particular item appears to fit this description will be at the sole discretion of the uniformed guard.

Proof of ownership may include:

- A memo from the AMS Officer stating that the property item to be removed is the employee's property, or
- Receipt of purchase.

USAID's contracted uniformed guards are required to review all property passes to ensure the following:

- The pass was signed by an authorized individual,
- The signature matches the one on file for that designated authorized individual,
- The description of material/articles match the items being removed, and
- The property pass is properly dated.

The AMS Officer is responsible for designating individuals within the B/IO with the authority to sign property passes. A signed designation must be sent to the Chief, SEC/ISP/DS, and AMS Officers must update the designation as changes occur. SEC maintains a copy of the listing of approved individuals authorized to sign property passes at USAID's 13 ½ Street and 14th Street guard post.

SEC personnel assigned to offsite facilities, to include SA-44 and Potomac Yards II, also maintain a current list of designated authorized personnel.

At SA-44, a copy of the listing of approved individuals is furnished to the U.S. Department of State Security Office. Questions and issues concerning property passes at SA-44 should be forwarded to the security officer assigned at that location.

565.3.10 Fingerprints

Effective Date: 05/24/2012

Prospective employees requesting fingerprints for the purpose of a personnel

security clearance may request to schedule an appointment by submitting a request directly to the **SECDomestic@usaid.gov** mailbox. The prospective employee must specify the reason why the fingerprints are needed and indicate if s/he has initiated the process required for completing the e-QIP (Electronic Questionnaire for Investigations Processing). Prospective employees must be able to furnish a valid government issued photo identification card (state-issued driver's license or U.S. Passport) in order to be fingerprinted. Fingerprinting appointments are scheduled Monday thru Friday according to the availability of the fingerprinting specialist.

USAID's Badge Office will not fingerprint institutional contractors to support investigations by other Federal agencies/departments.

565.3.11 Deliveries to USAID/W Facilities

Effective Date: 05/24/2012

USAID employees and staff at the Ronald Reagan Building, SA-44, and Potomac Yards II may pick up Federal Express, UPS, or other courier deliveries by reporting to the Front Desk to accept the delivery. USAID employees should ensure the courier has their office phone number and an alternate phone number to arrange for receipt of a package. Uniformed guards assigned to USAID/W will inspect all deliveries, including but not limited to courier mail and packages, parcels, bags, and flowers, prior to allowing these items to be introduced into the USAID space. In unusual or emergency circumstances, SEC may impose temporary restrictions on hand-carried items to ensure that materials are not introduced into USAID space.

Uniformed guards at all USAID/W buildings will not accept any packages under any circumstances.

All deliveries to the loading docks at the Ronald Reagan Building and SA-44 must be scheduled in advance through the Bureau for Management, Office of Management Services, Headquarters Management Division (M/MS/HMD) to arrange for mandatory screening upon arrival at the building's loading dock. Deliveries are not accepted at the general entrances.

Deliveries to the loading dock at Potomac Yards II must be coordinated through the U.S. Environmental Protection Agency (EPA), Office of Administration and Resources Management, Security Management Division, Security Operations Branch.

565.4 MANDATORY REFERENCES

565.4.1 External Mandatory References

Effective Date: 05/24/2012

a. 41 CFR 101-20.103, Physical Protection and Building Security

b. 12 FAM 500, Information Security

c. 12 FAM 683, Personal Digital Assistants

d. Federal Information Processing Standards, Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS PUB 201-1), March 2006

e. Homeland Security Presidential Directive-12 (HSPD-12), August 27, 2004

f. Interagency Security Committee: Use of Physical Security Performance Measures, 2009

g. Interagency Security Committee Standard: Physical Security Criteria for Federal Facilities, April 12, 2010

h. Presidential Directive, Subject: Upgrading Security at Federal Facilities, issued June 28, 1995

565.4.2 Internal Mandatory References

Effective Date: 05/24/2012

a. ADS 101, Agency Programs and Functions

b. ADS 103, Delegations of Authority

c. ADS 545, Information Systems Security

d. ADS 552, Classified Information Security Systems

e. ADS 561, Security Responsibilities

f. ADS 566, Personnel Security Investigations and Clearances

g. ADS 568, National Security Information Program

565.4.3 Mandatory Forms

Effective Date: 05/24/2012

a. AID Form 500-1, Request for Federal Identification Card/Facility Access Card

b. Form I-9, Employment Eligibility Verification

c. **GSA Optional Form 7**

565.5 ADDITIONAL HELP

Effective Date: 05/24/2012

There are no Additional Help documents for this chapter.

565.6 DEFINITIONS

Effective Date: 05/24/2012

See **ADS Glossary**

classified national security information (classified information)
Any data, file, paper, record, or computer screen containing information associated with the national defense or foreign relations of the United States and bearing the markings: Confidential, Secret, or Top Secret.
Information that has been determined pursuant to Executive Order (EO) 13526 or any predecessor order to require protection against unauthorized disclosure and is marked (Confidential, Secret, or Top Secret) to indicate its classified status when in documentary form. It is also referred to as classified information.

a. Confidential: Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

b. Secret: Information of which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

c. Top Secret: Information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.
(Chapters **545**, **552**, 565, and **568**)

Federal credential
A standardized form of identification as prescribed by Homeland Security Presidential Directive (HSPD-) 12 that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. (Chapter 565)

Facility Access Card (FAC)
An identification card issued to employees, detailees or contractors who do not qualify for a Federal ID card or who do not represent USAID to other agencies. (Chapter 565)

restricted space

An area where storage, processing, discussions, and handling of classified documents is authorized. (Chapters 565, **567**)

unrestricted space
An area where storage, processing, discussion, and handling of classified documents is not authorized. (Chapter 565)

565_100412